BUONE PRATICHE PER LA SICUREZZA INFORMATICA NEI SERVIZI SANITARI

Documento di indirizzo del Gruppo di Studio Nazionale sulla Cybersecurity nei servizi sanitari

Coordinamento:
Centro Nazionale per la Telemedicina e le Nuove Tecnologie Assistenziali, ISS – Dott. Francesco Gabbrielli
Centro Nazionale di Tecnologie Innovative in Sanità Pubblica, ISS – Ing. Mauro Grigioni

Membri del Gruppo
Prof. Fabrizio Baiardi (Università di Pisa), Dott.ssa Nunzia Ciardi (Direttore Polizia Postale e delle Comunicazioni), Prof. Claudio Cilli (Presidente del Rome Chapter ISACA), Prof. Alberto Marchetti Spaccamela (Università di Roma "La Sapienza"), Avv. Gabriele Faggioli e Avv. Maria Cristina Daga (CLUSIT, Politecnico di Milano), Ing. Giuliano Pozza (Presidente AISIS), Prof. Paolo Prinetto (Presidente CINI), Ing. Maurizio Rizzetto (AIIC), Ing. Francesco Vellucci (Digital SIT), Prof. Stefano Zanero (Politecnico di Milano).

La sicurezza informatica è un problema complesso che richiede specifiche soluzioni tecnologiche ed organizzative e non può essere improvvisata.
Essa deve essere sempre affrontata durante il progetto dei sistemi informativi ed adottando opportune tecniche di gestione dei sistemi durante tutta la loro vita. Tuttavia, comportamenti non adeguati degli utilizzatori semplificano gli attacchi anche a sistemi informativi che offrono una sicurezza elevata. È quindi necessario che il comportamento degli utilizzatori non generi situazioni pericolose che riducono la sicurezza intrinseca di un sistema mettendo in pericolo sia il sistema che i dati che esso gestisce. Per ottenere un contrasto ed una prevenzione efficace degli attacchi, le regole di buon comportamento devono essere diffuse ed adottate da tutto il personale delle strutture sanitarie, sia amministrativo che operativo. Per questo il documento suddivide le indicazioni in due paragrafi: il primo destinato a tutto il personale delle strutture sanitarie, il secondo con indicazioni utili ai gestori e responsabili di unità organizzative sia amministrative che operative.
Tale suddivisione è stata pensata al solo scopo di facilitare la lettura del presente documento anche a persone che non abbiamo specifiche conoscenze tecniche e non indica affatto una priorità di importanza o di urgenza. Tutte le indicazioni del presente documento sono quindi da ritenere ugualmente necessarie per incrementare il più possibile la difesa da cyberattacchi.
Il primo paragrafo riporta un semplice elenco, valido in generale per qualsiasi utilizzo di computer connessi in internet, di comportamenti corretti e scorretti ai fini della propria sicurezza.

REGOLE ESSENZIALI DI SICUREZZA INFORMATICA PER TUTTI

Cosa si deve fare:

- Dotarsi di una password sicura e cambiarla frequentemente.
- Conservare tutte le proprie password in modo sicuro.
- Cambiare immediatamente la password che sia stata comunicata a terzi o quando c'è il sospetto che non sia più segreta.
- Se ci viene richiesto di comunicare, anche a persone note, le proprie credenziali, prima di procedere contattare direttamente gli amministratori dei sistemi.

- Impostare uno screen-saver con richiesta di password o altro meccanismo di sicurezza per proteggere l'accesso alla propria postazione di lavoro nel caso di assenza anche temporanea.
- Spegnere la postazione di lavoro al termine dell'attività lavorativa giornaliera.
- Assicurarsi che sia presente un antivirus aggiornato sulla propria postazione di lavoro.
- Tenere aggiornati i computer con gli aggiornamenti dei relativi sistemi operativi.
- Controllare con l'antivirus i file o i supporti provenienti dall'esterno.
- Configurare il programma di posta elettronica in modo che non esegua automaticamente gli allegati.

Cosa NON si deve fare

- Lasciare aperta una sessione di lavoro sui server centrali e abbandonare la postazione.
- Comunicare la propria password ad altri a voce o via e-mail.
- Conservare la password su quaderni, agende, post-it o simili (magari attaccati sul computer o sul monitor).
- Salvare la password sul browser, sull'applicazione, sulla posta elettronica, o quando proposto dal sistema operativo, per non doverla digitare all'accesso.
- Lasciare impostata la password di default fornita dal costruttore di apparati o servizi.
- Aprire e/o rispondere a e-mail di cui non si conosce il mittente e che non erano state richieste, o che contengono allegati inusuali e/o collegamenti a indirizzi web.
- Cliccare su icone che appaiono negli allegati di posta, anche se dall'apparenza innocua, ad esempio che ricordano applicazioni associate ad immagini o musica.

BUONE PRATICHE PER TUTTO IL PERSONALE DEI SERVIZI SANITARI

Gestione delle credenziali: accorgimenti per tutto il personale

Scelta della password

- la password deve essere composta da almeno otto caratteri, oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la password non deve contenere riferimenti aventi attinenza con la vita privata o professionale facilmente riconducibili all'utente (evitare ad es. nome, cognome, data di nascita, numero di telefono, codice fiscale, luogo di nascita, nome di parenti ecc.);
- le password non devono essere parole di senso comune presenti sul dizionario;
- la password non deve contenere una serie consecutiva di soli numeri o di sole lettere;
- la password, nel caso in cui lo strumento elettronico lo permetta, deve essere preferibilmente composta da una sequenza di lettere, numeri e caratteri speciali (es. di caratteri speciali: &;@*§ ? % £=@ $); si sottolinea l'importanza di inserire dei caratteri speciali con lo scopo di rendere meno facile agli algoritmi l'intercettazione;
- la password non deve essere costituita da una sequenza ovvia sulla tastiera (es. qwerty, 123456);
- la password deve essere diversa dalle ultime 2-3;
- la password deve essere facile da ricordare per l'utente.

Cautele per la segretezza della password

- utilizzare sempre esclusivamente le proprie credenziali di autenticazione;
- non condividere la propria password con altre persone;
- mantenere e custodire le proprie password con la dovuta riservatezza;

- evitare di scrivere le proprie password su foglietti di carta o agende, a meno che tali supporti cartacei non vengano custoditi in cassetti o armadi chiusi a chiave;
- nel digitare sulla tastiera la password, prestare attenzione ad eventuali sguardi indiscreti;
- comunicare tempestivamente al responsabile o all'amministratore di sistema eventuali dubbi sulla segretezza della password;
- modificare immediatamente la password nel caso sia stato necessario fornire le credenziali ai tecnici intervenuti per la manutenzione del computer o del software.

Modifica della password

- modificare la password temporanea assegnata dall'amministratore, al primo utilizzo (primo log-on);
- cambiare immediatamente la password nel caso si sospetti abbia perso il requisito della segretezza;
- modificare la password di accesso alle applicazioni utilizzate per il trattamento di dati personali almeno ogni sei mesi;
- in caso di trattamento di dati sensibili (es. dati personali inerenti lo stato di salute) e giudiziari la password deve essere modificata almeno ogni tre mesi;
- comunicare all'incaricato della custodia delle credenziali la modifica, consegnandogli in busta chiusa le proprie credenziali.

Difendersi dal phishing

- non digitare le proprie credenziali su siti web raggiunti tramite link presenti su messaggi e-mail o altri documenti;
- non aprire messaggi di posta provenienti da utenti sconosciuti;
- non comunicare la propria password a nessuno, nemmeno all'amministratore di sistema;
- inoltrare al proprio Servizio Informativo i messaggi che si ritengono sospetti e cancellarli dalla propria casella.

Gestione delle stazioni di lavoro: per tutto il personale

Custodia della stazione di lavoro

- evitare di lasciare incustodito e accessibile lo strumento elettronico durante una sessione di lavoro che comporti trattamento di dati personali;
- proteggere la stazione di lavoro attraverso cui si accede a sessioni di trattamento di informazioni riservate, utilizzando o key locks, password di qualità o screen saver (da attivare su richiesta o dopo un tempo prestabilito di inattività), nel caso in cui ci si assenti temporaneamente dall'ufficio;
- al termine della sessione di lavoro sui server centrali, effettuare la procedura di disconnessione ("logoff"/"logout"/"esci");
- al termine della sessione sulla stazione di lavoro, effettuare la procedura di arresto del sistema ed attendere che sia terminata prima di lasciare l'ufficio.

Credenziali delle stazioni di lavoro

Nei casi in cui:

- siano mantenute informazioni di interesse comune sulla propria stazione di lavoro,
- la propria stazione di lavoro sia l'unica abilitata ad accedere ad uno specifico servizio,

il responsabile della stazione di lavoro è consapevole che deve essere garantito l'accesso alla stazione stessa in caso di assenza. L'accesso può essere garantito o attraverso la nomina di un collega fiduciario, opportunamente informato delle credenziali della stazione di lavoro o attraverso la consegna delle credenziali stesse al 'Custode delle credenziali' della propria struttura.

Prevenzione dei virus informatici

- verificare il regolare funzionamento della procedura automatica di aggiornamento del programma antivirus, al fine di accertarsi che la procedura sia andata a buon fine;
- utilizzare il software rispettando le istruzioni del fornitore;
- verificare, tramite adeguato programma antivirus, i file, il software e i dispositivi di memorizzazione rimovibili (hard disk esterni, chiavette USB, ecc.) provenienti dall'esterno, prima del loro utilizzo;
- segnalare tempestivamente al personale tecnico preposto qualsiasi presenza di virus sospetta che pregiudichi o abbia pregiudicato il sistema di sicurezza delle informazioni;
- nello scaricare dalla rete Internet programmi (es. software open source; freeware, shareware ecc.) e documenti (testi e tabelle che possono contenere dei "virus macro") necessari allo svolgimento della propria attività lavorativa, utilizzare unicamente i siti delle case produttrici dei medesimi o i link che esse stesse propongono sul loro sito;
- nell' utilizzo della posta elettronica, evitare di aprire allegati che contengono un'estensione doppia o con estensione VBS, SHS, PIF, EXE, COM o BAT (a meno che non attesi e provenienti da mittente conosciuto e di fiducia);
- se si ricevono e-mail non richieste o con contenuti pubblicitari, evitare di seguire i collegamenti a indirizzi Web eventualmente presenti nel testo delle e-mail;
- nel caso si riceva un messaggio di e-mail da una persona conosciuta, ma con un contenuto insolito, effettuare un controllo con il mittente prima di aprire l'eventuale allegato; infatti alcuni virus sono in grado di trasmettere messaggi con allegati che sembrano spediti da mittenti conosciuti;
- evitare di cliccare su icone dall'apparenza innocua che ricordano applicazioni associate ad immagini o musica, mostrate dagli allegati di posta elettronica in quanto possono nascondere "worm".

Politica di aggiornamenti software

- ove non possibile un aggiornamento automatico, controllare almeno mensilmente la disponibilità di aggiornamenti e provvedere alla loro installazione;
- segnalare tempestivamente al personale tecnico preposto qualsiasi vulnerabilità o attività sospetta che pregiudichi o abbia pregiudicato il sistema di sicurezza delle informazioni o la presenza di virus sulla propria postazione di lavoro;
- non effettuare gli aggiornamenti dei software installati sul computer o di nuove versioni del sistema operativo, senza prima informarsi presso il personale tecnico preposto della compatibilità con gli applicativi centralizzati utilizzati.

Telefoni

Sono considerati strumenti informatici che possono dare accesso ad informazioni riservate o strategiche, quindi:

- non lasciare il telefono a disposizione di persone estranee;
- valutare l'opportunità di inserire il lucchetto elettronico all'uscita dal lavoro o in caso di assenza prolungata;
- non comunicare il codice per la gestione della segreteria telefonica e per lo sblocco del telefono a persone estranee.

Stampanti

Se si dispone di stampanti di rete o condivise:

- ritirare immediatamente le stampe contenenti informazioni riservate o strategiche;
- non lasciare operazioni di stampa in sospeso sul computer;
- assicurarsi che la stampante sia in linea e funzionante prima di inviare in stampa i documenti;

- non comunicare a persone estranee la password di accesso alla stampante o altri parametri di configurazione che potrebbero consentire la stampa da remoto.

Gestione del materiale: per tutto il personale

Gestione del materiale di output

- se non utilizzati e quando ci si assenta dall'ufficio, provvedere a custodire in armadio o cassetto muniti di serratura i supporti removibili (es. chiavette USB, cd) contenenti informazioni riservate o strategiche;
- controllare attentamente lo stato delle stampe di documenti riservati e rimuovere immediatamente tali copie dalla stampante, onde evitare che personale non autorizzato abbia accesso alle informazioni;
- provvedere a rendere inintelligibili eventuali stampe non andate a buon fine.

Gestione del materiale cartaceo

- conservare i supporti cartacei contenenti dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati stessi (stanze, armadi, cassetti chiusi a chiave);
- se si è in attesa di un documento contenente informazioni riservate via fax, non lasciare incustodito l'apparecchio del fax ma rimuovere immediatamente il documento.

BUONE PRATICHE PER GESTORI E RESPONSABILI DI UNITÀ ORGANIZZATIVE

Gestione delle credenziali: accorgimenti per i responsabili di unità organizzative

Il custode delle credenziali

All'interno di ogni ufficio è buona pratica individuare uno o più custodi delle credenziali che hanno il compito di conservare, in luogo sicuro (armadio o cassetto chiuso a chiave, cassaforte, ecc.), le credenziali del personale afferente alla struttura. Le credenziali da conservare possono essere quelle di accesso agli applicativi centralizzati, ma anche quelle per l'accesso al proprio computer o alla propria casella di posta elettronica forniti dall'organizzazione.

Ogni coppia di credenziali è consegnata dal proprietario al custode in busta chiusa riportante il proprio nominativo e il sistema al quale si riferiscono.

Per l'accesso alle singole credenziali così custodite deve essere redatta una procedura a cura del responsabile della struttura che preveda le modalità di consegna della relativa busta chiusa sia su richiesta del legittimo proprietario, sia su richiesta del responsabile in caso di urgenti e improrogabili esigenze di servizio.

Modalità di comunicazione delle credenziali

Le credenziali generate a seguito di specifica richiesta, sono inserite dall'amministratore di sistema di SIAF in una busta chiusa da portare in segreteria. La busta viene allegata ad una nota di accompagnamento da inviare, tramite posta interna, al responsabile che ha effettuato la richiesta, che si occuperà della consegna della busta, ancora chiusa, all'interessato.

Gestione delle stazioni di lavoro: per i responsabili di unità organizzative

Custodia della stazione di lavoro

- accertarsi che il backup dei dati e documenti essenziali, sulle stazioni di lavoro anche portatili, sia effettuato regolarmente (almeno una volta alla settimana) e sempre tramite il servizio di file service fornito dalla propria organizzazione oppure, ove impossibilitati, su CD o altro supporto esterno dedicato a questo scopo e opportunamente protetto;
- preferire, nelle macchine o strumenti particolarmente sensibili, il collegamento tramite cavo e non WIFI al fine di poter ridurre ulteriori canali di accesso soggetti ad attacchi cyber.

Prevenzione dei virus informatici

- verificare che il software antivirus in dotazione sia correttamente installato;
- accertarsi che sia configurata la protezione permanente;
- accertarsi che sia configurato l'aggiornamento automatico via rete;
- verificare che il sistema operativo sia configurato in modo da rendere possibile visualizzare l'estensione dei file: tale accorgimento rende più difficile il mascheramento da parte di file potenzialmente pericolosi (programmi EXE e script di vario tipo) che impiegano estensioni doppie (es. "leggimi.txt.vbs" oppure "logo.jpg.exe");
- disporre immediatamente la bonifica da virus delle stazioni che si rivelino o vengano segnalate come infette;
- verificare che il programma di posta elettronica sia configurato in modo tale che non esegua automaticamente gli allegati.

Politica di aggiornamenti software

- configurare, ove possibile, l'esecuzione automatica degli aggiornamenti del sistema operativo, ovvero
- configurare, ove possibile, lo scaricamento automatico dalla rete degli aggiornamenti (patch) del sistema operativo ed eseguire l'installazione non appena disponibile.

Gestione del materiale: per i responsabili di unità organizzative

Gestione del materiale di output

- verificare che i supporti removibili (es. chiavette USB, cd) contenenti informazioni riservate o strategiche siano correttamente custoditi in arredi muniti di serratura, in caso di inutilizzo o di assenza dall'ufficio del personale.

Gestione del materiale cartaceo

- verificare che i supporti cartacei contenenti dati personali siano conservati in modo da evitare che siano accessibili a persone non autorizzate al trattamento dei dati (stanze o arredi, chiusi a chiave).

Gestione delle apparecchiature dismesse

- le informazioni classificate come "riservate" (dati personali, dati sensibili ecc.) devono essere cancellate in maniera definitiva dai dispositivi di memorizzazione, prima che le apparecchiature vengano dismesse (trasferite per essere riutilizzate da altri utenti, riciclate o smaltite);
- il semplice comando di cancellazione o di formattazione non è spesso sufficiente per garantire una cancellazione permanente dei dati. Sono infatti disponibili diversi modi per recuperare i documenti che sono stati cancellati, anche dopo la formattazione dell'hard disk. Occorre prestare particolare

attenzione quando si gestiscono dati personali e sensibili, informazioni strategiche o coperte da riservatezza;

- per quanto concerne le vecchie stazioni di lavoro da dismettere, è compito di ciascun assegnatario provvedere alla permanente distruzione delle informazioni critiche e alla disinstallazione del software con licenza installato sulle stazioni di lavoro:
  - nel caso di reimpiego o di riciclo la cancellazione sicura può essere effettuata tramite uno dei programmi di 'wiping' disponibili in rete, una formattazione a basso livello, oppure la demagnetizzazione,
  - nel caso di smaltimento la cancellazione può anche prevedere la distruzione dei supporti tramite sistemi di punzonatura o deformazione meccanica, distruzione fisica o disintegrazione, demagnetizzazione ad alta intensità;
- per quanto riguarda invece i server, gli storage system, le cartucce, è compito dell'organizzazione provvedere alla cancellazione permanente delle informazioni riservate. Per garantire l'impossibilità di recupero dei dati, si utilizzano tecniche di formattazione profonda, oppure si provvede alla distruzione fisica dell'apparecchiatura, dopo aver completato la procedura di scarico del bene inventariale.

Formazione del personale

Il primo e più efficace strumento per il gestore che abbia il compito di promuovere la cultura della prevenzione di attacchi informatici è senza dubbio l'adeguata programmazione della formazione specifica per il proprio personale. Il personale deve imparare a proteggere il sistema sanitario, il paziente e se stesso.
La formazione deve essere progettata ed erogata per trasferire i principi di funzionamento di un computer e delle reti di computer, senza entrare nei dettagli tecnici; deve mostrare la realtà delle attività di attacco e dei loro utilizzi criminali rispetto agli usi illeciti dei dati sanitari; deve infine suggerire la messa in atto di accorgimenti e comportamenti idonei a prevenire il più possibile l'intrusione nei sistemi informatici comunemente in uso in ambito sanitario.

L'apprendimento viene favorito quando tale formazione viene svolta in stretta correlazione con le attività quotidiane del personale a cui viene destinata, descrivendo per ciascuna attività i rischi e per ogni rischio i principali scenari di attacco e le relative contromisure, sia in fase di prevenzione che sotto attacco.
Quindi, nel caso dei dipendenti e operatori, i primi scenari su cui progettare eventi formativi sono:

- Divulgazione di dati a Persone non autorizzate:
  - individui che cercano di ottenere informazioni riservate per telefono o di persona,
  - e-mail malevole (Phishing),
  - utilizzo incauto dei social (whatsapp, facebook, ecc.),
  - accesso alle cartelle sanitarie e a dispositivi medici in rete,
  - malware scaricato sul proprio dispositivo,
  - smarrimento/furto di dispositivi non protetti,
  - furto delle credenziali.
- Alterazione di dati e generazione di malfunzionamenti:
  - malware scaricato sul proprio dispositivo,
  - e-mail malevole (Ransomware),
  - accesso alle cartelle sanitarie e a dispositivi medici in rete,
  - furto delle credenziali.